Governing an Accountable Privacy Program

Scott Taylor
Merck & Co., Inc.
Chief Privacy Officer

June 23, 2022
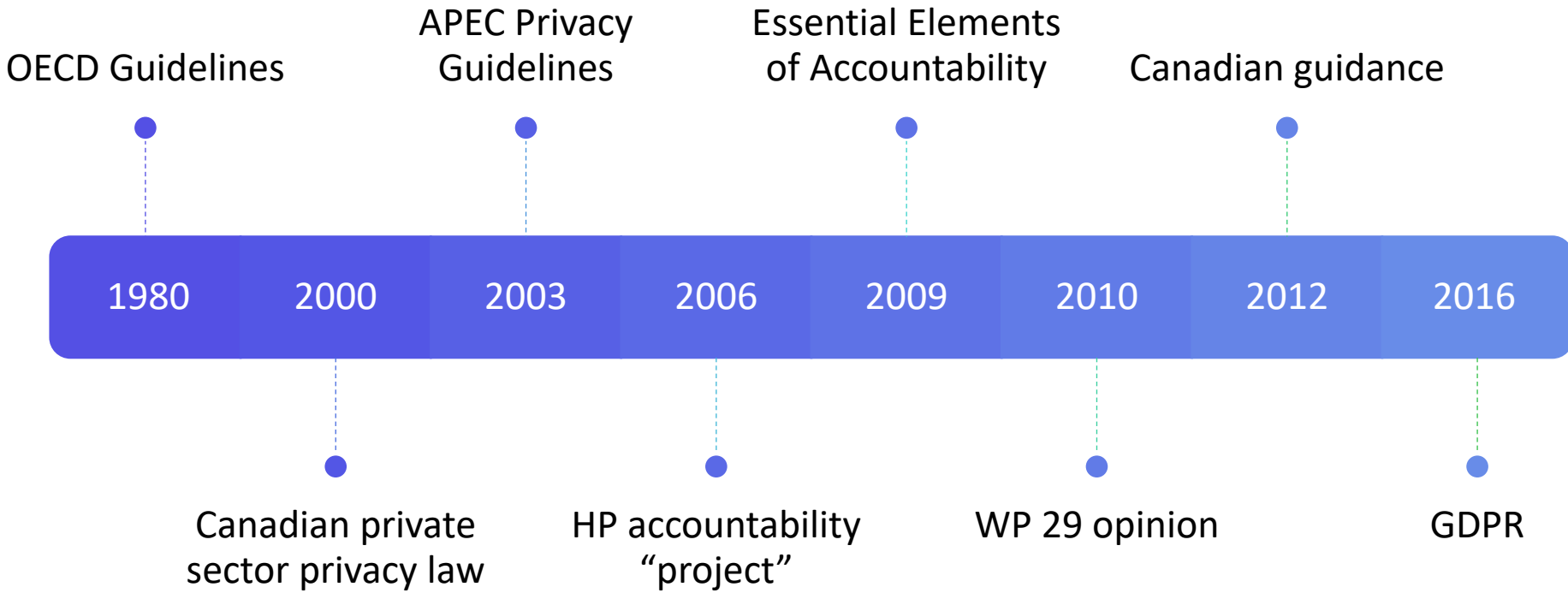
Accountability Made Simple

Responsible

Answerable for being responsible

IAF

Accountability Timeline

OECD Guidelines

APEC Privacy Guidelines

Essential Elements of Accountability

Canadian guidance

| 1980 | 2000 | 2003 | 2006 | 2009 | 2010 | 2012 | 2016 |

Canadian private sector privacy law

HP accountability "project"

WP 29 opinion

GDPR

IAF

Demonstrable Accountability Elements

Organizational commitment to fair processing demonstrable accountability and the adoption of internal policies consistent with external criteria and established fair processing principles.
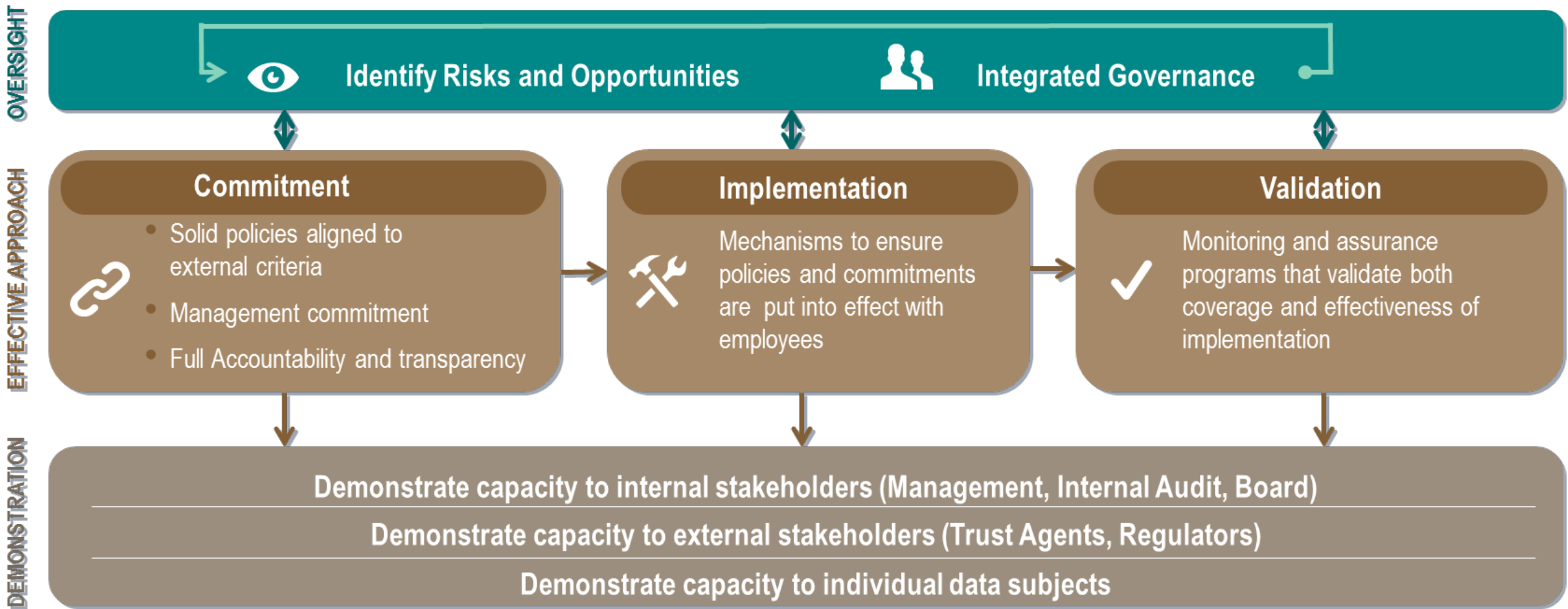
Mechanisms to put fair processing policies into effect, including risk based adverse impact assessments, tools, training and education.

Internal review processes that assess higher risk FIPAs and the overall fair processing program.
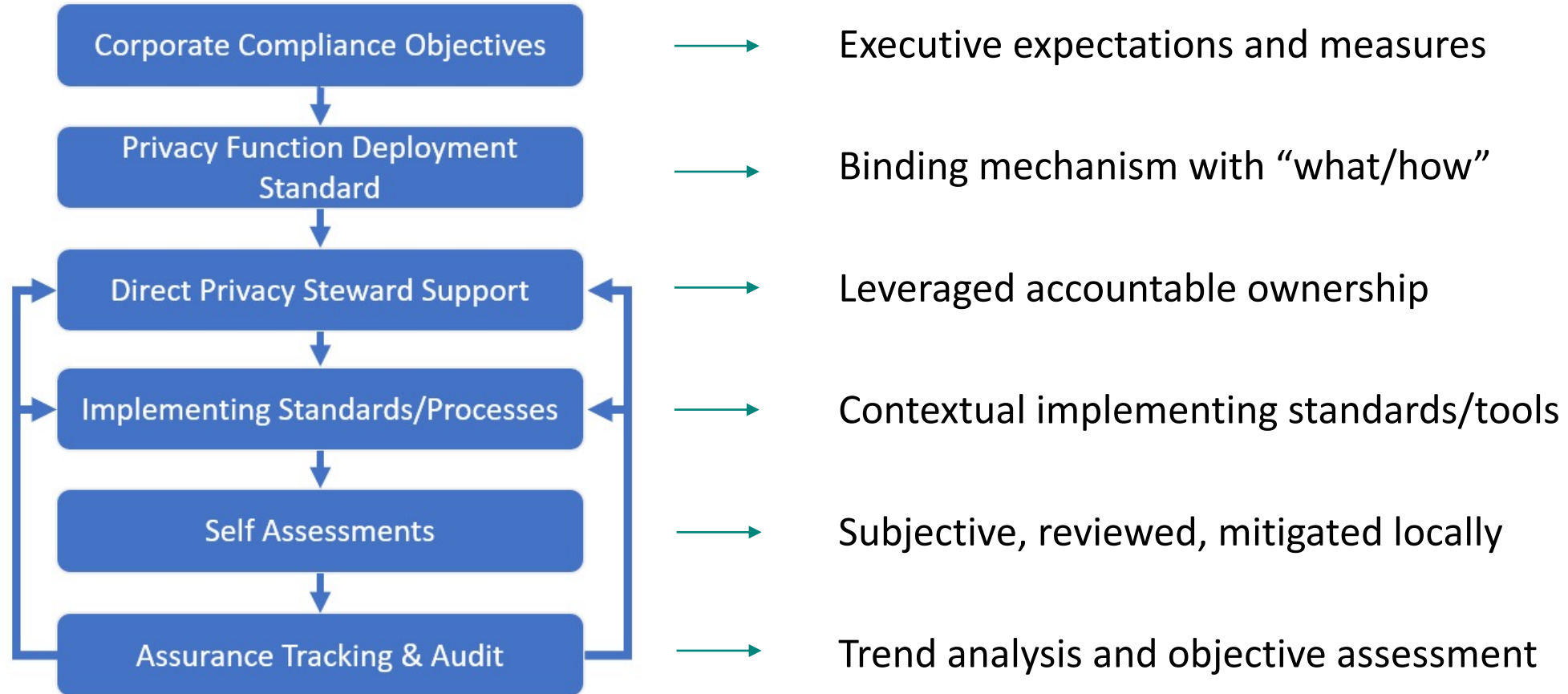
Individual and organizational demonstrability and mechanisms for individual participation.

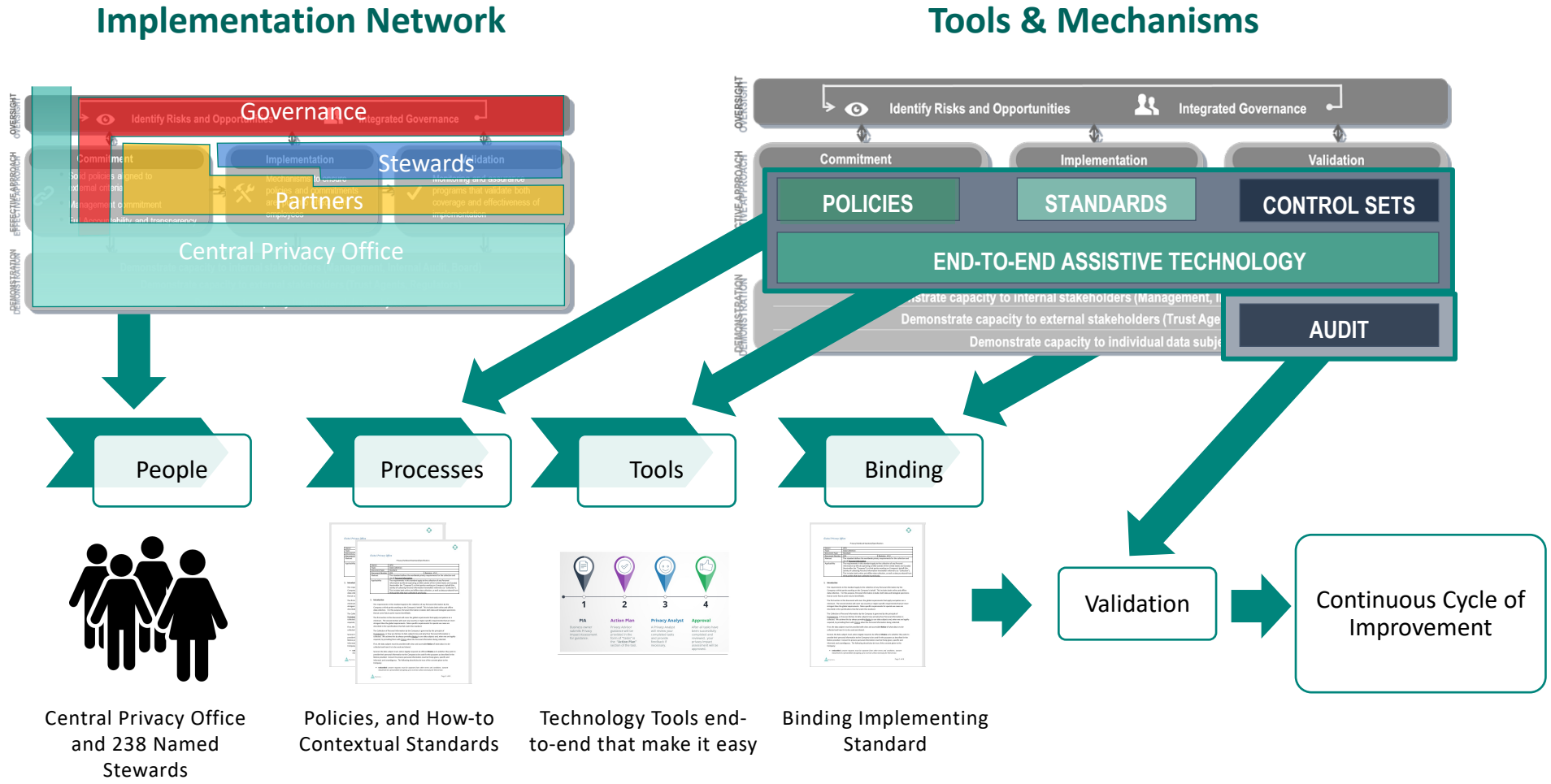Means for remediation and external enforcement.

IAF

Merck's Strategic Privacy Framework – Meeting Regulator Expectations

OVERSIGHT

Identify Risks and Opportunities   Integrated Governance

EFFECTIVE APPROACH

Commitment
- Solid policies aligned to external criteria
- Management commitment
- Full Accountability and transparency

Implementation
Mechanisms to ensure policies and commitments are put into effect with employees

Validation
Monitoring and assurance programs that validate both coverage and effectiveness of implementation

DEMONSTRATION

Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)

Demonstrate capacity to external stakeholders (Trust Agents, Regulators)

Demonstrate capacity to individual data subjects

INVENTING FOR LIFE

Putting the Privacy Program Into Effect

Corporate Compliance Objectives	→	Executive expectations and measures
Privacy Function Deployment Standard	→	Binding mechanism with "what/how"
Direct Privacy Steward Support	→	Leveraged accountable ownership
Implementing Standards/Processes	→	Contextual implementing standards/tools
Self Assessments	→	Subjective, reviewed, mitigated locally
Assurance Tracking & Audit	→	Trend analysis and objective assessment

Key Program Components & Mechanisms

Implementation Network

Governance

Stewards

Partners

Central Privacy Office

Tools & Mechanisms

OVERSIGHT — Identify Risks and Opportunities — Integrated Governance

Commitment	Implementation	Validation
POLICIES	STANDARDS	CONTROL SETS

END-TO-END ASSISTIVE TECHNOLOGY

Demonstrate capacity to internal stakeholders (Management, I...
Demonstrate capacity to external stakeholders (Trust Age...
Demonstrate capacity to individual data subj...

AUDIT

| People | Processes | Tools | Binding | | Validation | Continuous Cycle of Improvement |

Central Privacy Office and 238 Named Stewards

Policies, and How-to Contextual Standards

Technology Tools end-to-end that make it easy

Binding Implementing Standard

Health of the Program

Data Determines the Health of the Program

In addition to the direct Regulator reviews and certifications, our focus, in every aspect of the new program, is to gain insights and real-time data:

- Training

- Privacy Impact Assessments

- Supplier Diligence and Assessments

- Contracts

- Incident Management

- Data Subject Rights

- Program Self-Assessments/Audits

By instrumenting these processes, we continue to improve our ability to spot trends, mitigate risks, and deploy our resources in the most critical areas. It is also the core of an ability to demonstrate.

Incident Monitoring

We have live feeds of all incidents – ensuring immediate actions and ability to meet regulatory requirements.
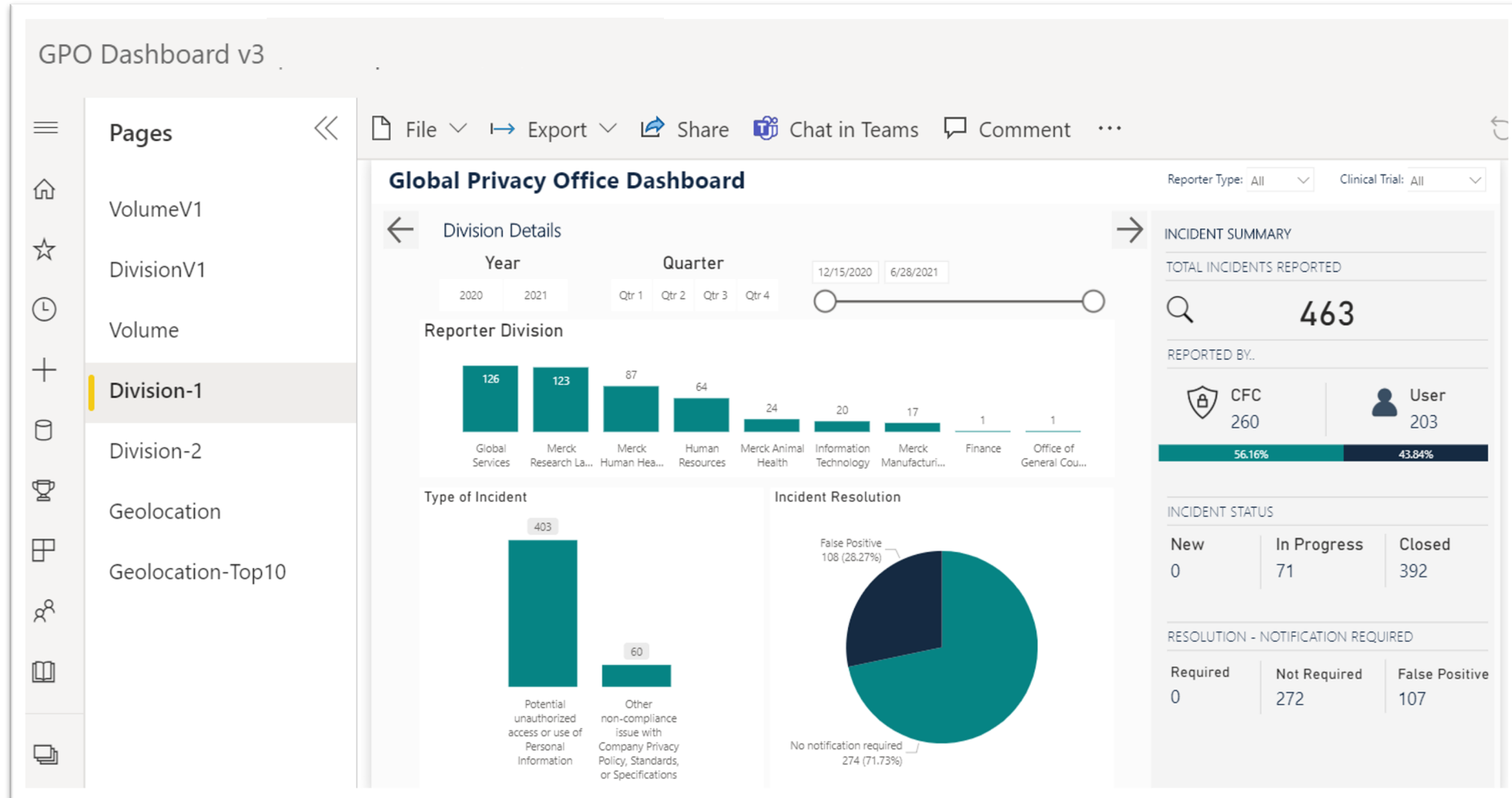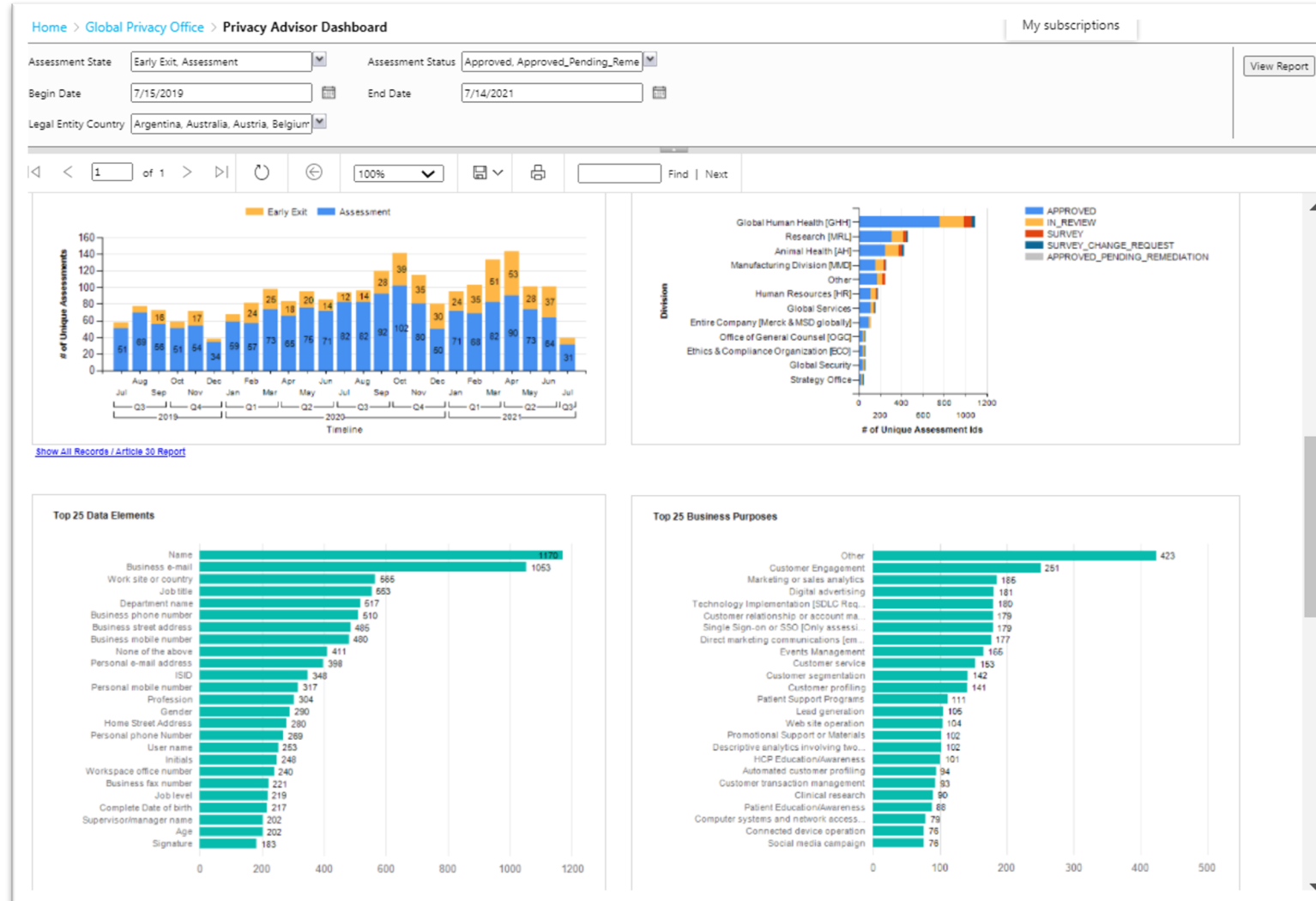
Third-Party Diligence Monitoring

We have live feeds of all supplier diligence – reducing third-party risk and meeting regulatory requirements.
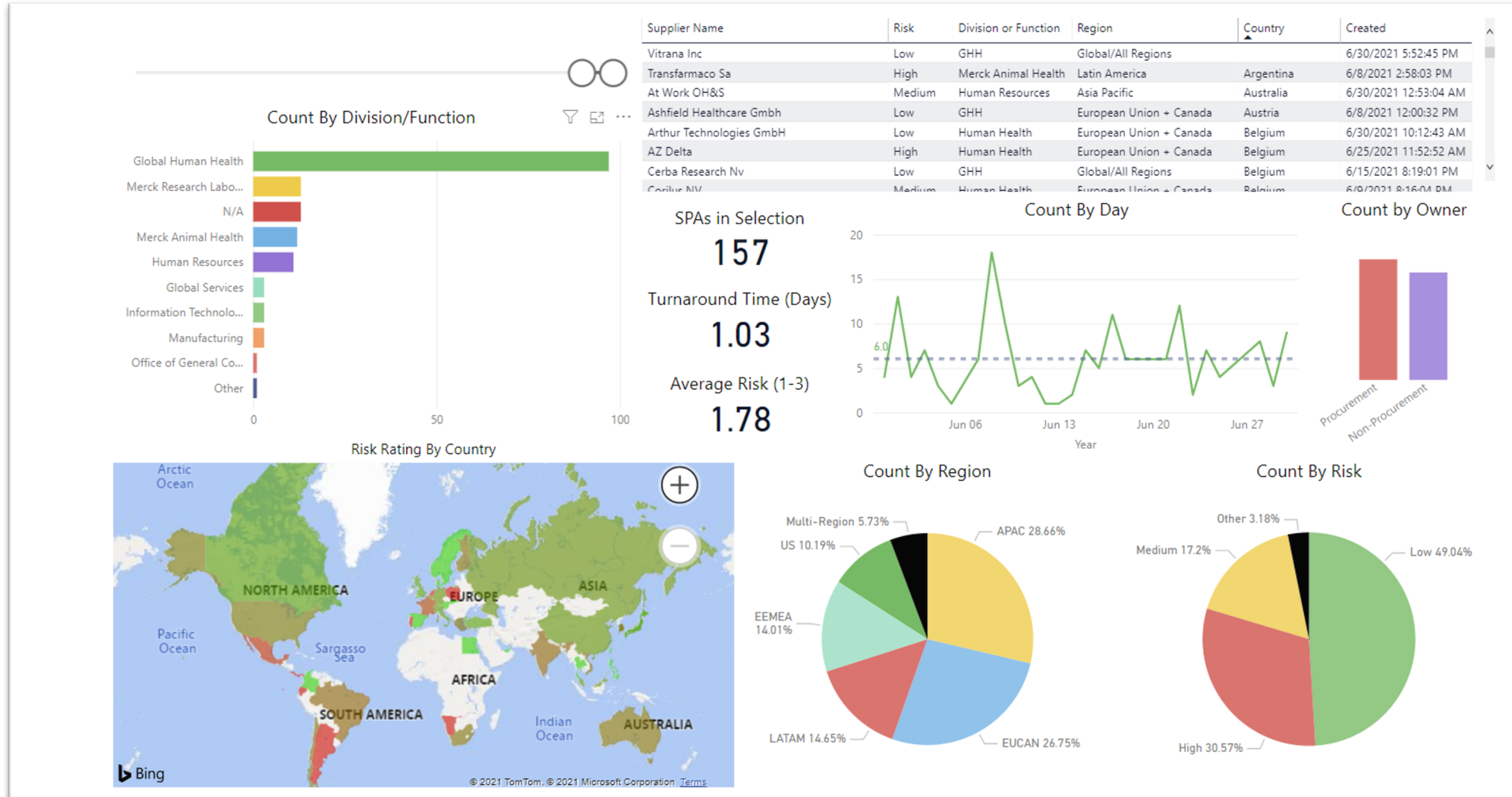
# Privacy Impact Assessment Monitoring

We have live feeds of all privacy impact assessments – ensuring we reduce risk and meet our reporting requirements.

Program Deployment Maturity Monitoring

- Privacy Stewards complete self-assessments at least 1X/Year
  - Measures of perceived maturity
  - CAPAs with Local Leadership Teams
- The Global Privacy Office monitors and tracks trends
  - Targeted support
  - Uplifting Privacy Steward capabilities
- The Global Privacy Office provides Audit Prep
- MCAAS (Internal Audit) audits
  - Measures actual maturity
- Continual program improvement/refinement

Average Regional Maturity

Region	Value
APAC	4.77
EEMEA	4.52
EUCAN	4.89
LATAM	4.67
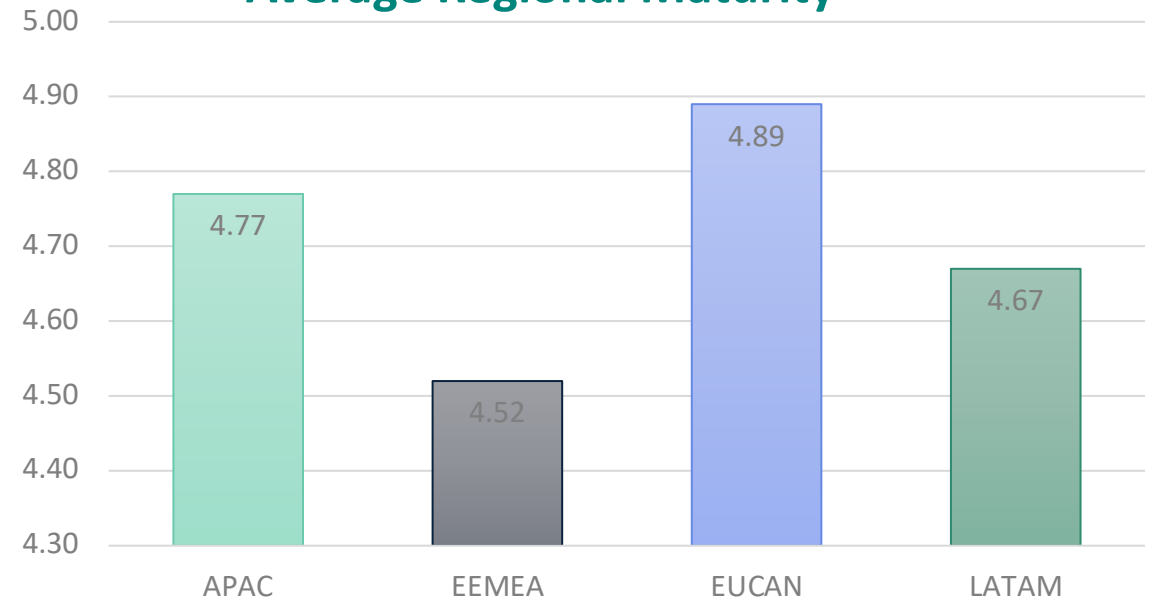
- Overall Maturity is rated from a low of 1 to a high of 5.
- Privacy Program maturity is highest in EUCAN as they have had more time to deploy.

Governing Via Data
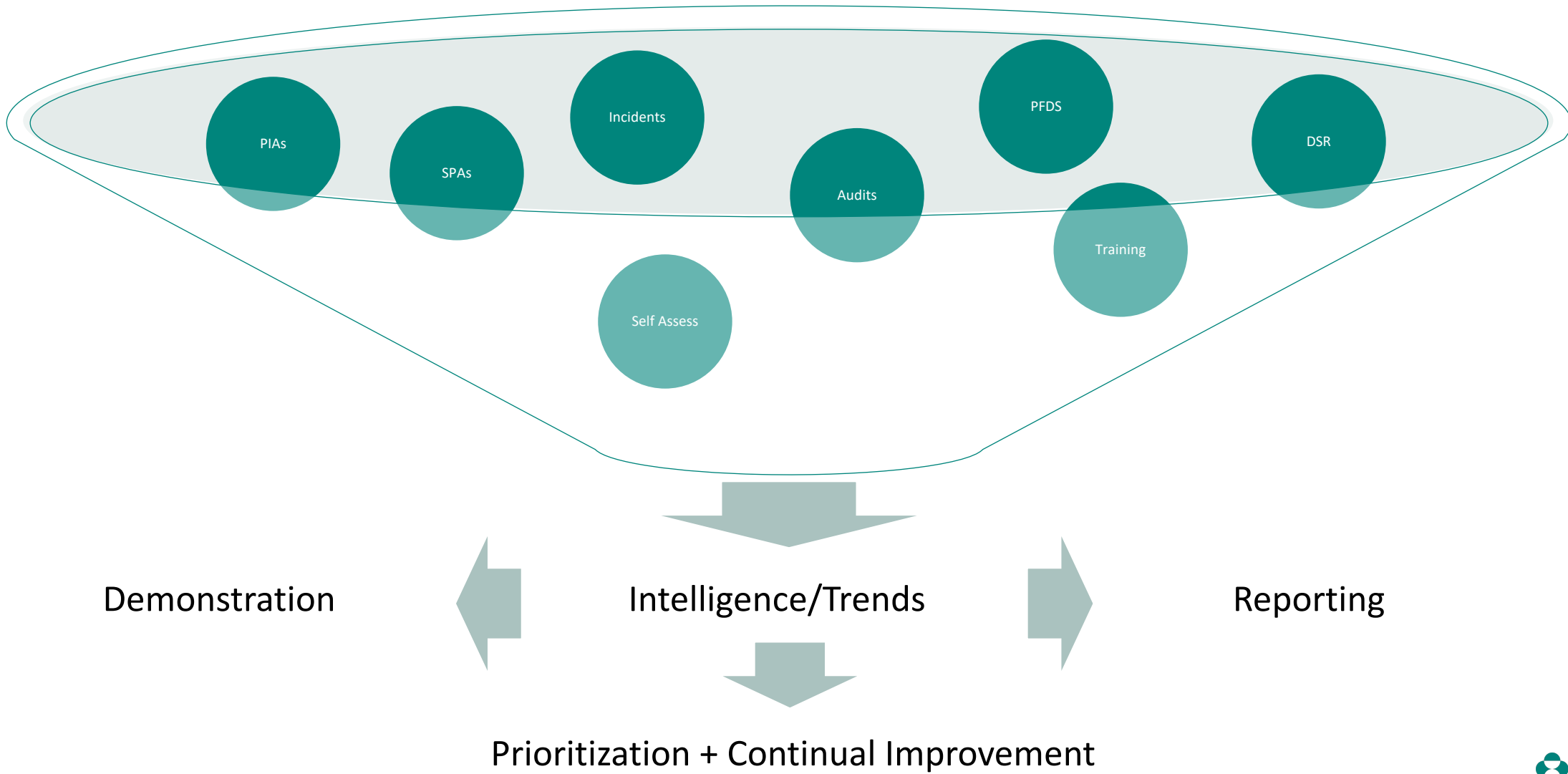
Accountability & Demonstration

Accountability

Accountability can come in many forms

- What it is not:

  - Pretty slides and empty words on a page

- What it is:

  - A willingness to share what sits behind the words

  - Transparency

  - Balancing the tensions in a responsible, fair, and just manner

  - Openness to scrutiny and a commitment to addressing concerns

  - A continuous cycle of data-driven learning and improvement

Questions?